NTIA Coordinated Disclosure Working Group for Safety Industries: DRAFT Scoping Document

Problem Statement:

"Our dependence on connected software is growing faster than our ability to secure it; increasingly affecting public safety and human life. This is where bits & bytes meet flesh & blood". – IamTheCavalry.org

Regarding software vulnerabilities, safety industries carry some of the highest stakes, but enjoy the least experience with coordinated disclosure issues.

Because of the elevated stakes and the highly personalized impacts of failures, the need to drive high trust, high collaboration models is increased. Here are a few impacts we discussed:

- **Life & Limb Impact:** The consequences of failure can include public safety and human life for (ourselves and) our loved ones - in contrast to highly replaceable, recoverable losses of Credit Cards Numbers or Passwords.
- **Trust Affecting GDP & Economic Stability:** Safety related industries represent double-digit contributors to national economies. Any crisis of confidence in (e.g. connected vehicles) could have a material impact on national GDP. Whereas a breach from one traditional Retailer may temporarily rattle trust in their brand, high consequence failures in safety are more likely to rattle confidence in the cadre of industry participants.
- **Perverse Effects of Shaken Trust:** Ironically, a consequence of fear toward modern devices and vehicle could prevent adoption of otherwise safety-enhancing technological advances.

Marc Andreessen pronounced, "Software is eating the world" - that every company, regardless of what they do, is becoming a software company. We see this manifest as our cars, our medical devices, our homes, our trains and planes – are increasingly connected. As we add the benefits of connected software in the Internet of Things, with those benefits come new accidents and adversaries. While the software industry and researchers have struggled to consistently find common ground for high trust, high collaboration models over the last 15-20 years, we cannot afford such a mean-time-to-collaboration in the safety critical industries.

The bad news: Most of these safety industries are already exposed to new classes of accidents and adversaries, and are nascent in their experience with Coordinated Disclosure.

The good news: These safety industries are not yet entrenched in their positions toward vulnerability collaborations, and can benefit from many of the lessons learned, hard earned wisdom, and advances made over the years by exemplars.

We can be safer, sooner, together.

Related Background / Further Reading:

IATC 5 Star Cyber Safety Framework

https://www.iamthecavalry.org/domains/automotive/5star/

IATC Position on Disclosure for Safety Issues

"*Those concerned with public safety and human life should take sufficient care to avoid inadvertently putting them at risk."*

https://www.iamthecavalry.org/about/disclosure/

Related ISOs (International Standards Organization)

- 2700x Information Security Management
  http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
- 30111 Vulnerability Handling Process
  http://www.iso.org/iso/catalogue_detail.htm?csnumber=53231
- 29147 Vulnerability Disclosure
  http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170
- 26262 Vehicle Functional Safety
  http://www.iso.org/iso/catalogue_detail.htm?csnumber=54591
- 14971 Medical Device Risk Safety
  http://www.iso.org/iso/catalogue_detail?csnumber=38193
  - Third party software has to be traceable and validated
- 13485 Medical Device Computer Systems
- Industrial Controls?
- Aviation?

Microsoft Security Development Lifecycle

- https://www.microsoft.com/en-us/sdl/
- BlueHat

Fault Tree Analysis & Threat Modeling (STRIDE)

- https://en.wikipedia.org/wiki/Fault_tree_analysis
- https://en.wikipedia.org/wiki/Hazard_analysis

"Disclosure" has baggage (Rainforest Puppy, [No | Full | Responsible | Coordinated] Disclosure)

- e.g. https://en.wikipedia.org/wiki/RFPolicy

Approaches to Address & Initial Steps Worth Taking

- Produce Document: "How Safety is different from traditional security practices"
  IamTheCavalry (dot org) has a framework worth starting from:
  - Different Adversaries
  - Different Consequences: Life and Safety, not privacy
  - Different Operational Contexts: Migratory, device is it's own perimeter, etc
  - Different Composition: HW/FW/SW stacks and supply chains

    - Different Time Scales: 30 years, not 30 days/weeks/months
    - Different Economics: Who pays, eg. MSSP to monitor in real-time
    - Different Scope/Boundaries of Risk (GDP, Industry Stability, “Public Health”/ “Public Good”/”Commons”)
    - Different Emotional/Visceral Public Impact (Trust, Safety, “Flesh & Blood”)
    - Different maturity points on their “Cyber Journey” (Year 0 in Preparedness & Culture)
- Produce Document: Glossary/Lexicon Mapping
    - Words matter. Better communication means better results.
    - Apparently common nouns and verbs take on radically different meanings across industries. (E.g, Safety)
    - Different people and different fields use different terminology.
        - Researchers need to understand that terms like “risk”, “exploit”, “vulnerability”, and “overflow” may have very different meanings when you speak to someone from the auto industry, public utilities, or video game services. Steps should be taken to minimize communication issues.
        - Companies, in all fields, need to be aware that vulnerability disclosure reports coming from the computer security field may not use the same terminology found in their own fields.
- Produce Document: WHY high trust, high coordination is of benefit (versus WHAT to do or HOW to do it):
    - For Researchers
    - For Manufacturer/Corporations
    - For Affected public/Customers
    - ***NOTE: This could/should link with/reference the Awareness & Adoption Working Group’s fruits.***
- Produce Document: Mapping between existing Industry Frames or models
    - E.g. Fault Tree Analysis versus Threat Modeling
    - E.g. 5-Star Cyber Safety Framework for Automotive https://www.iamthecavalry.org/domains/automotive/5star/

        - Anticipate and avoid failure
        - Take help anticipating and avoiding failure
        - Detect and learn from failure
        - Respond promptly and agilely to failure
        - Contain and isolate failure
- Produce Document: Introduction to IT Risk for Safety Industries.
- Produce Document: Consumer’s Bill of Rights for Safety Expectations and Assurances
- Produce Diagram(s): Single Page Model or Venn Diagrams for aforementioned mappings
- Produce Document: Motivations and Methods of Researchers

Open Topics / Parking Lot:

- Effective and safe methods of access to large, rare, and/or cost prohibitive devices/technologies for Coordinated Research and Remediation.
- Robust, clear, well-known escalation and mediation paths for when impasses are reached (e.g. DHS ICS-CERT can and has helped with Medical Device impasses)
- The emerging role of Cyber Insurance for kinetic impacts/damages
- Emerging Liability models for the Internet of things
- Chilling effects of dated and/or counterproductive computer laws – and newly proposed ones… I.e. how can we adapt laws to better prosecute true adversaries without dampening/discouraging true allies and teammates for the public good and public safety
- Sensational “Stunt Hacking” has triggered both action and less obvious “anti-body” polarizing effects, which can damage trust and run counter to high trust, high collaboration models.
- Probably lots more… which might you suggest?

Working Group Live Call(s) Participants

Joshua Corman (I Am The Cavalry)
Allen Householder (CERT)
Amanda Craig (Microsoft)
Drew Mitnick (Access Now)
Tara Hairston (Honda)
Beau Woods (I Am The Cavalry)
Graham Watson (DOT Volpe)
Tom Cross (Drawbridge Networks)
Steve Christey Coley (MITRE)
Neal Krawetz (Hacker Factor)
Joe Klein (Disrupt6)